(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 315 394 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
28.05.2003 Bulletin 2003/22

(51) Int Cl.7: **H04Q 7/38**, H04L 12/56,
H04L 12/28

(21) Application number: 02396173.3

(22) Date of filing: 20.11.2002

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LU MC NL PT SE SK TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: 22.11.2001 FI 20012283

(71) Applicant: **Sonera Oyj**
00510 Helsinki (FI)

(72) Inventors:
- **Korhonen, Jouni**
  11100 Riihimäki (FI)
- **Keisala, Iikka**
  01600 Vantaa (FI)
- **Väänänen, Kai**
  02940 Espoo (FI)

(74) Representative: **Simmelvuo, Markku et al**
Papula Oy,
P.O. Box 981
00101 Helsinki (FI)

(54) Short-distance wireless connections in a telecommunication network

(57) The present invention relates to a method for authentication of short-distance wireless connection setup and encryption of a connection set up between two or more mobile terminals in a digital mobile communication network. According to the invention, the MSISDN subscriber number of the first terminal is utilized for identification of the first terminal by the second terminal, a short message inquiry is sent from the terminal selected as master to the gateway server, a random number is generated by the gateway server in response to the short message inquiry, the random number generated is sent in a response to the short message inquiry from the gateway server to both terminals, and the short-distance wireless connection set up between the terminals is encrypted by utilizing the aforesaid random number and encryption keys stored on the user identity modules of the terminals.

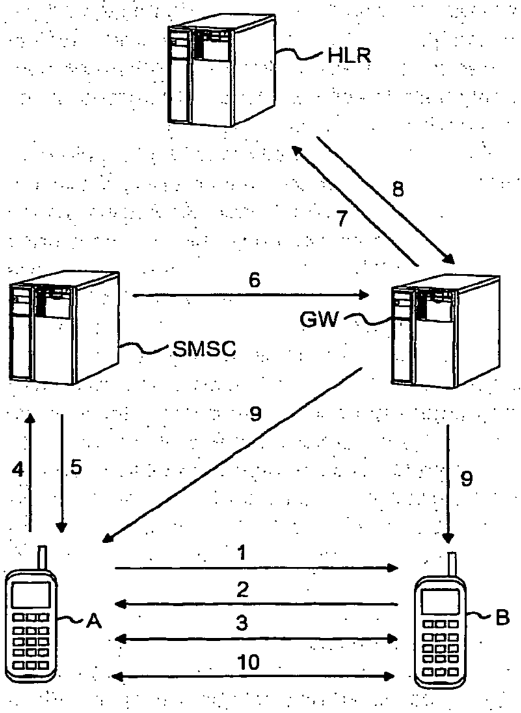

Fig. 1

Description

FIELD OF THE INVENTION

[0001] The present invention relates to telecommunication. In particular, the invention relates to a new and sophisticated method for authenticating short-distance wireless connection setup, encrypting a connection set up and transmitting presence and location data over short-distance wireless connections.

PRIOR ART

[0002] The popularity of wireless terminals, such as e.g. mobile stations has increased at a fast tempo during the past ten years. In addition, short-distance wireless connections are being introduced. 'Short-distance wireless connection' refers to a connection based on short-range radio link technology with a maximum range of the order of ten meters, primarily intended for use inside buildings and preferably so that the transmitter and receiver are situated in the same room, said connection permitting communication of information among more than two devices at a time. In particular, short-distance wireless connections are designed to replace cable connections, which are in use at present. Further, short-distance wireless connections are designed to replace infrared links, which involve the disadvantage of a short operating range, typically only a couple of meters. Moreover, infrared links require accurate alignment, and the transmission path between transmitter and receiver must be free of obstacles. In addition, an infrared connection only permits communication of information between two devices at a time.

[0003] One of these short-distance wireless connection technologies is the Bluetooth technology. Bluetooth uses a 2.4 GHz ISM (Industrial Scientific Medicine) band for data transfer. In most countries, this frequency band lies between 2400-2483,5 MHz. The frequency band is divided into 1 MHz channels. The protocol used by Bluetooth is a combination of circuit switching and packet switching. Data transfer is implemented using a spread spectrum based on frequency hopping. The maximum operating range is normally of the order of ten meters. By increasing the transmission power, it is possible to increase the range up to one hundred meters. Connections may be bilateral or multilateral. Bluetooth is preferably implemented as a microcircuit, which is either integrated directly in the device utilizing it or installed afterwards as an expansion card.

[0004] However, current implementations of short-distance wireless connections involve many drawbacks that reduce their service value. For example, setting up temporary, so-called ad-hoc networks between Bluetooth terminals is at present no user-friendly or visually observable process because present terminals provided with Bluetooth are very uninformative when connections and temporary networks are being set up. For instance, the other party is only shown as a row of figures resembling a MAC code (Media Access Control). Further, today's Bluetooth technology provides no solution to the problem of distribution of encryption keys. Moreover, the transmission of presence and/or location information is a problem with current short-distance wireless connections. In current solutions, for example, users have to update their status themselves every time when it changes. Furthermore, current implementations provide no possibility to associate location data with presence data.

OBJECT OF THE INVENTION

[0005] The object of the present invention is to disclose a new type of method that eliminates the above-mentioned drawbacks or at least significantly alleviates them. A specific object of the invention is to disclose a method that enables authentication of short-distance wireless connection setup and encryption of a connection set up as well as transmission of presence and location data over short-distance wireless connections.

BRIEF DESCRIPTION OF THE INVENTION

[0006] In the present invention for authentication of short-distance wireless connection setup and encryption of a connection set up between two or more mobile terminals in a digital mobile communication network comprising a number of mobile terminals and a gateway server, each of said mobile terminals comprising a subscriber identity module and a short-distance wireless connection module, a short-distance wireless connection setup inquiry is sent from a first terminal to a second terminal. Next, the first terminal is identified by the second terminal. On the basis of a predetermined selection parameter, one of the terminals is selected as master and the other as slave. The digital mobile communication network is e.g. a GSM network (Global System for Mobile Communication) or a UMTS network (Universal Mobile Telecommunications System). It is to be noted that the aforesaid digital mobile communication network and temporary short-distance wireless network consisting of terminals utilizing short-distance wireless connections are entities independent of each other.

[0007] According to the invention, the MSISDN subscriber number (Mobile Subscriber ISDN) of the first terminal is sent together with the short-distance wireless connection setup inquiry to the second terminal. Further according to the invention, the said MSISDN subscriber number of the first terminal is utilized for identification of the first terminal by the second terminal. Further according to the invention, a short message inquiry is sent from the terminal selected as master to the gateway server. Further according to the invention, a random number is generated by the gateway server in response to the short message inquiry. Further according to the invention, the random number generated is sent in a response to the short message inquiry from the gateway server to both terminals. Further according to the invention, encryption of the short-distance wireless connection set up between the terminals is performed using the aforesaid random number and encryption keys stored on the user identity modules of the terminals.

[0008] In an embodiment of the invention, the random number is produced by generating it using the gateway server.

[0009] In an embodiment of the invention, the random number is produced by sending a random number request from the gateway server to a Home Location Register provided in connection with the aforesaid mobile communication network and sending the random number in question from the Home Location Register to the gateway server in response to the request.

[0010] In an embodiment of the invention, the target address of the short message inquiry comprises the subscriber number of the gateway server.

[0011] In an embodiment of the invention, the information contained in the short message inquiry comprises the MSISDN subscriber number of the terminal selected as slave.

[0012] In an embodiment of the invention, the MSISDN subscriber numbers of the terminals are used as a selection parameter.

[0013] In an embodiment of the invention, for identification of the first terminal by the second terminal, the MSISDN subscriber number of the first terminal is presented on the display of the second terminal.

[0014] In an embodiment of the invention, the short-distance wireless connection set up between the terminals is encrypted by using a predetermined symmetrical-key encryption technique.

[0015] In an embodiment of the invention, the short-distance wireless connection is a Bluetooth connection.

[0016] In an embodiment of the invention, the short-distance wireless connection is an IrDA connection (Infrared Data Association).

[0017] In an embodiment of the invention, the subscriber identity module is a USIM module (Universal Subscriber Identity Module).

[0018] In an embodiment of the invention, the USIM module comprises a dedicated storage location, which comprises predetermined connection parameters associated with short-distance wireless connection setup.

[0019] In an embodiment of the invention, the connection parameters comprise the MSISDN subscriber numbers of those terminals with which short-distance wireless connection setup is allowed.

[0020] In an embodiment of the invention, the connection parameters comprise the MSISDN subscriber numbers of those terminals with which short-distance wireless connection setup is not allowed.

[0021] In an embodiment of the invention, the connection parameters comprise the MSISDN subscriber numbers of those terminals with which short-distance wireless connection setup is only allowed after a separate interactive verification inquiry.

[0022] In the present invention for the transmission of presence and location information between two or more terminals in a telecommunication network, said telecommunication network comprising a number of terminals and a number of base stations, said terminals and base stations communicating with each other using short-distance wireless connections, a first terminal is disposed within the coverage area of a first base station and a short-distance wireless connection is set up between the first terminal and the first base station.

[0023] According to the invention, a location server is provided in connection with the telecommunication network. Further according to the invention, terminal-specific presence data, comprising an identifier of the first base station and an indication of whether the first terminal in question is present within the area of the telecommunication network, is transmitted automatically from the first base station to the location server. Further according to the invention, terminal-specific location data, comprising an identifier of the first base station and information indicating the base station in whose coverage area the first terminal in question is located, is transmitted automatically from the first base station to the location server. Further according to the invention, the presence data and location data for the first terminal are automatically transmitted from the location server to one or more other terminals. Further according to the invention, when the first terminal is moving so that its location data changes, said location data is updated automatically in the location server and the updated location data is transmitted to one or more other terminals. Further according to the invention, when the first terminal is moving so that its presence data changes, said presence data is updated automatically in the location server and the updated location data is transmitted to one or more other terminals.

[0024] In an embodiment of the invention, the SIP protocol (Session Initiation Protocol) is utilized in transmitting the location data. The SIP protocol is a protocol standardized by the IETF (Internet Engineering Task Force), intended for the initiation of an interactive user session.

[0025] In an embodiment of the invention, the SIP protocol is utilized in transmitting the presence data.

[0026] In an embodiment of the invention, the information regarding the base station in whose coverage area a given terminal is located, which is included in the location data, comprises an additional parameter definable by the user of the terminal in question.

[0027] In an embodiment of the invention, when the terminal is simultaneously located in the coverage areas of two or more different base stations, the terminal in question is sent a notification about the situation as well as a list of the base stations concerned, on the basis of which the base station to be transmitted in the location data is selected interactively by the user of the terminal.

[0028] In an embodiment of the invention, the short-distance wireless connections are Bluetooth connections.

[0029] In an embodiment of the invention, the telecommunication network is a WLAN network (Wireless Local Network).

[0030] As compared with prior-art technology, the present invention provides the advantage that it facilitates the setup of temporary short-distance wireless networks between terminals by making network setup more user-friendly and visually clear. The invention enables terminals trying to enter into the network to be identified by their MSISDN subscriber numbers. Further, the invention makes it possible to display to the user the plain-language names corresponding to these MSISDN subscriber numbers if said MSISDN subscriber numbers are stored in the memory of the subscriber identity module of the user's terminal.

[0031] Further, the invention solves the problem of distribution of encryption keys by utilizing between terminals an encryption system of the type used in present digital mobile communication networks together with the encryption key already existing on the subscriber identity module.

[0032] Further, the invention provides a more user-friendly presence service, in which the presence data and location data are updated automatically without requiring the user to personally update the data every time the status is changed. Moreover, the invention allows the use of several additional parameters in the presence service.

LIST OF ILLUSTRATIONS

[0033] In the following, the invention will be described in detail by the aid of embodiment examples with reference to the attached drawings, wherein

Fig. 1 is a diagrammatic illustration of a method according to the invention, and

Fig. 2 is a diagrammatic illustration of a method according to the invention.

DETAILED DESCRIPTION OF THE INVENTION

[0034] Fig. 1 presents by way of example a diagrammatic illustration of a method according to the invention for authentication of short-distance wireless connection setup and for encryption of a connection set up between two or more mobile communication terminals in a digital mobile communication network, which comprises mobile communication terminals A and B provided with a Bluetooth function, and a gateway server GW, a home location register HLR and a short message switching center SMSC.

[0035] At step 1, A starts the process of setting up a Bluetooth connection. B receives a connection setup inquiry and performs a master-slave comparison. After the comparison, B sends a notification of the result to A, step 2. At step 3, a connection exists between A and B, but so far unauthenticated and unreliable. In the master-slave comparison carried out, A is selected as master on the basis of the MSISDN subscriber numbers of A and B, so A sends a SMS short message into the mobile communication network. The target address of the message is the gateway server's GW target number used as service number. The message content consists of the MSISDN subscriber number of B. At step 4, the message is transmitted to the short message switching center, and at step 5 an eventual acknowledgement of receipt of the message is transmitted to A.

[0036] At step 6, the short message switching center SMSC directs the message to the gateway server GW on the basis of the target address included in the message. The gateway server GW requests a random number for A from the home location register HLR, step 7. At step 8, the home location register HLR returns a random number to the gateway server GW. Instead of the home location register HLR, a random number can also be generated e.g. directly by the gateway server GW. As a result of the request, the gateway server GW returns the same random number in a short message to both A and B, step 9. At step 10, the random number received is taken into use and the connection between A and B is encrypted using a symmetrical-key technique known in itself.

[0037] Fig. 2 presents a diagram illustrating by way of example a method according to the invention for transmitting presence and location data between two or more terminals in a telecommunication network, said telecommunication network comprising a number of terminals A, B and C, a number of base stations BS and a location server DB. The terminals A, B, C and the base stations BS communicate with each other using Bluetooth connections. Fig. 2 shows terminals of three different types. At steps 1 and 2, a terminal and a Bluetooth base station are signaling, in other words, they find each other and set up a Bluetooth connection. At steps 3 and 4, the Bluetooth base station transmits data to the location server to indicate that a given client has entered the coverage area of this base station. In steps 5 and 6, which represent an alternative to steps 3 and 4, the clients are connected to the location server via a permanent connection. After this, all active users of the location service are automatically updated with information giving the actual locations of the terminals. If necessary, authentication can be carried out using the method illustrated in Fig. 1.

[0038] The invention is not limited to the embodiment examples described above; instead, many variations are possible within the scope of the inventive concept defined in the claims.

Claims

1. Method for authentication of short-distance wire-

less connection setup and encryption of a connection set up between two or more mobile communication terminals in a digital mobile communication network comprising a number of mobile terminals and a gateway server, each of said mobile terminals comprising a subscriber identity module and a short-distance wireless connection module, said method comprising the steps of:

sending a short-distance wireless connection setup inquiry from a first terminal to a second terminal,
identification of the first terminal by the second terminal, and
selecting one of the terminals as master and the other as slave on the basis of a predetermined selection parameter,

characterized in that the method further comprises the steps of:

sending the MSISDN subscriber number (Mobile Subscriber ISDN) of the first terminal together with the short-distance wireless connection setup inquiry to the second terminal,
utilizing the said MSISDN subscriber number of the first terminal for identification of the first terminal by the second terminal,
sending a short message inquiry from the terminal selected as master to the gateway server,
generation of a random number by the gateway server in response to the short message inquiry,
sending the random number thus generated in a response to the short message inquiry from the gateway server to both terminals, and
encrypting the short-distance wireless connection thus set up between the terminals, using the aforesaid random number and encryption keys stored on the user identity modules of the terminals.

2. Method according to claim 1, **characterized in that** the random number is produced by generating it using the gateway server.

3. Method according to claim 1, **characterized in that** the random number is produced by sending a random number request from the gateway server to a home location register provided in connection with the mobile communication network and sending the random number in question from the home location register to the gateway server in response to the request.

4. Method according to claim 1, 2 or 3, **characterized in that** the target address of the short message inquiry comprises the target number of the gateway server.

5. Method according to claim 1, 2, 3 or 4, **characterized in that** the information contained in the short message inquiry comprises the MSISDN subscriber number of the terminal selected as slave.

6. Method according to claim 1, 2, 3, 4 or 5, **characterized in that** the MSISDN subscriber numbers of the terminals are used as a selection parameter.

7. Method according to claim 1, 2, 3, 4 5 or 6, **characterized in that**, for identification of the first terminal by the second terminal, the MSISDN subscriber number of the first terminal is presented on the display of the second terminal.

8. Method according to claim 1, 2, 3, 4, 5, 6 or 7, **characterized in that** the short-distance wireless connection set up between the terminals is encrypted by using a predetermined symmetrical-key encryption technique.

9. Method according to claim 1, 2, 3, 4, 5, 6 or 7, the short-distance wireless connection is a Bluetooth connection.

10. Method according to claim 1, 2, 3, 4, 5, 6, 7 or 8, **characterized in that** the short-distance wireless connection is an IrDA connection.

11. Method according to claim 1, 2, 3, 4, 5, 6, 7, 8, 9 or 10, **characterized in that** the subscriber identity module is a USIM module.

12. Method according to claim 11, **characterized in that** the USIM module comprises a dedicated storage location, which comprises predetermined connection parameters associated with short-distance wireless connection setup.

13. Method according to claim 12, **characterized in that** the connection parameters comprise the MSISDN subscriber numbers of those terminals with which short-distance wireless connection setup is allowed.

14. Method according to claim 12 or 13, **characterized in that** the connection parameters comprise the MSISDN subscriber numbers of those terminals with which short-distance wireless connection setup is not allowed.

15. Method according to claim 12, 13 or 14, **characterized in that** the connection parameters comprise the MSISDN subscriber numbers of those terminals with which short-distance wireless connection setup is only allowed after a separate interactive veri-

fication inquiry.

16. Method for the transmission of presence and location data between two or more terminals in a telecommunication network, said telecommunication network comprising a number of terminals and a number of base stations, said terminals and base stations communicating with each other using short-distance wireless connections, said method comprising the steps of:

- disposing a first terminal within the coverage area of a first base station, and
- setting up a short-distance wireless connection between the first terminal and the first base station,

characterized in that the method further comprises the steps of:

- providing a location server in connection with the telecommunication network,
- automatically transmitting terminal-specific presence data, comprising an identifier of the first base station and an indication of whether the first terminal in question is present within the area of the telecommunication network, from the first base station to the location server,
- automatically transmitting terminal-specific location data, comprising an identifier of the first base station and information indicating the base station within whose coverage area the first terminal in question is located, from the first base station to the location server,
- automatically transmitting the presence data and location data for the first terminal from the location server to one or more other terminals,
- automatically updating the location data for the first terminal in the location server when said terminal is moving so that its location data changes, and transmitting the updated location data to one or more other terminals, and
- automatically updating the presence data for the first terminal in the location server when said terminal is moving so that its presence data changes, and transmitting the updated location data to one or more other terminals.

17. Method according to claim 16, **characterized in that** the SIP protocol is utilized in transmitting the location data.

18. Method according to claim 16 or 17, **characterized in that** the SIP protocol is utilized in transmitting the presence data.

19. Method according to claim 16, 17 or 18, **characterized in that** the information regarding the base station in whose coverage area a given terminal is located, which is included in the location data, comprises an additional parameter definable by the user of the terminal in question.

20. Method according to claim 16, 17, 18, 19 or 20, **characterized in that**, when the terminal is simultaneously located in the coverage areas of two or more different base stations, the terminal in question is sent a notification about the situation as well as a list of the base stations concerned, on the basis of which the base station to be transmitted in the location data is selected interactively by the user of the terminal.

21. Method according to claim 16, 17, 18, 19 or 20, **characterized in that** the short-distance wireless connections are Bluetooth connections.

22. Method according to claim 16, 17, 18, 19 or 20, **characterized in that** the telecommunication network is a WLAN network.

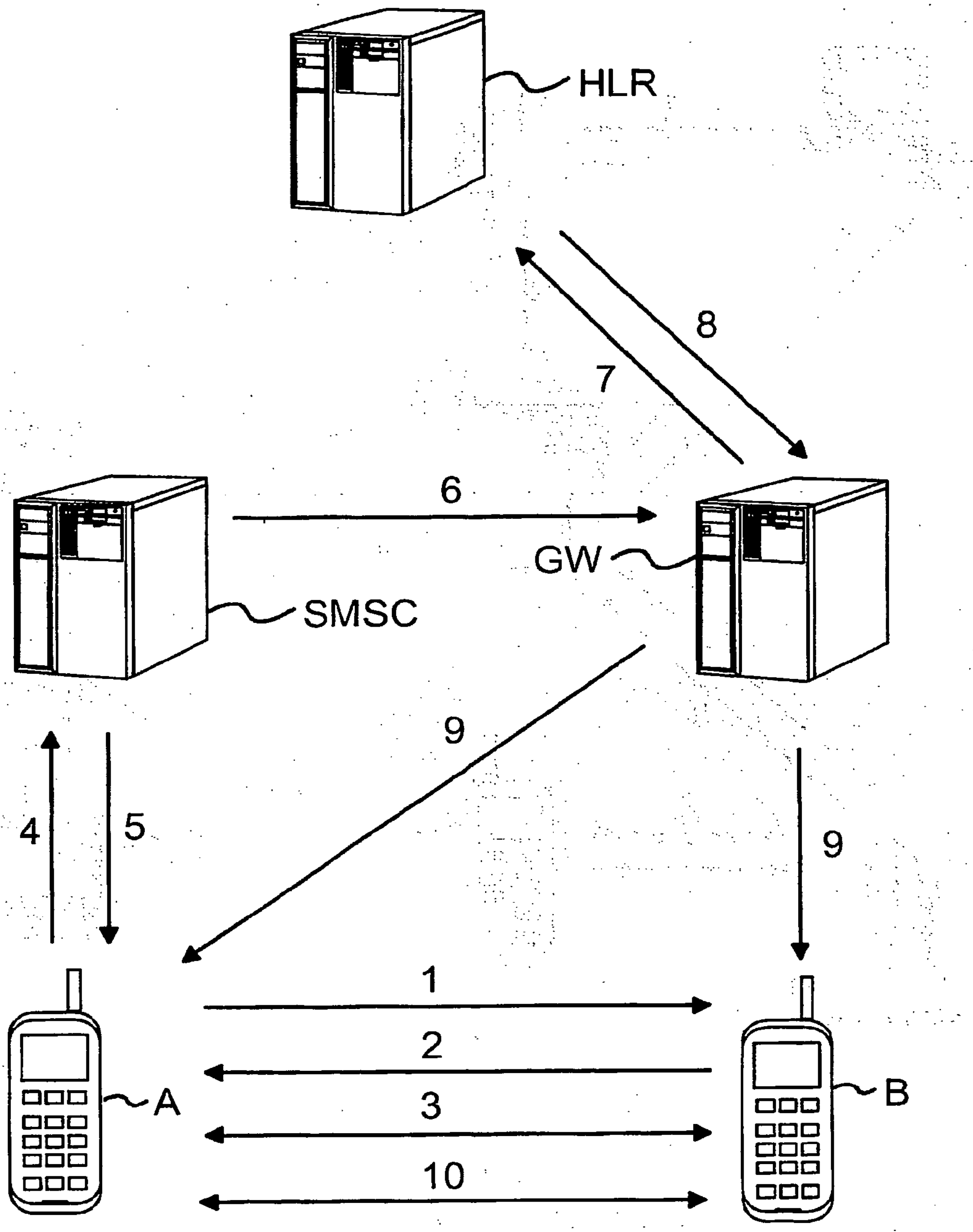

Fig. 1

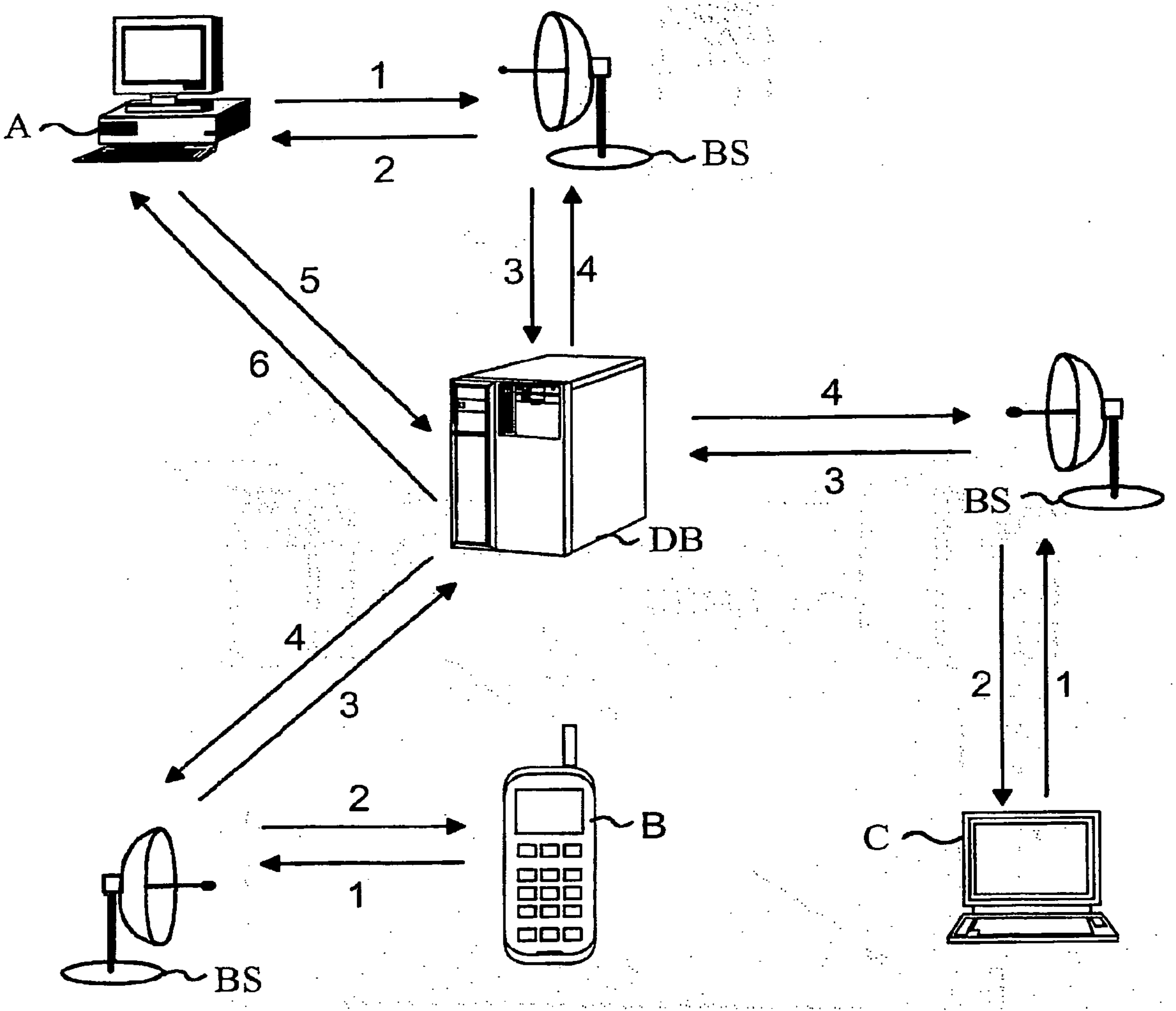

Fig. 2